

REMARKS

This Request for Reconsideration is filed in response to the Office Action of July 31, 2007 in which claims 20-23 were rejected as being unpatentably obvious over *Geiger et al* (WO 2000/72149) in view of *Proust et al* (U.S. 7,151,922).

In the *Geiger* reference, a list of application programs (33) is stored and, for each application program, a digital fingerprint of that application program. Upon execution of an application program, a check (23, 206) is made of the list for an entry that includes the digital fingerprint of the application program. The application is executed if the digital fingerprint is present. Otherwise, digital signature verification (26, 220) is performed for the application program if the digital fingerprint is not present in the list (see Abstract).

The Examiner's analysis reads the claimed limitation of "before allowing the software module to take control of the terminal, the terminal communicates via the mobile communication with the software provider" onto the disclosure of the *Geiger* reference at page 4, lines 8-15 and Fig. 3, steps 200-230. This is incorrect because just before the quoted phrase from the presently claimed claim 20, there appears the following phrase "said software module already stored on a removable memory unit connected to the terminal and ready for use." Everything in Fig. 3 of the *Geiger* reference except for step 201 takes place in the terminal device 10. In other words, although the download of an applet could be considered by the Examiner to be a form of "communicating" in a mobile communication system, this interpretation must also admit by its very terms that the software module is not already stored in the terminal 10 and ready to use. This is critically important for the present invention because the "communicating" is quite different from that disclosed by *Geiger* as will be appreciated by reference to the transmitting and receiving steps of claim 20. These are best illustrated by reference to Fig. 2 of the present application at steps 203 and 209.

The transmit step 203 of Fig. 2 takes place in the terminal and follows a hash step 201 that also takes place in the terminal. The steps 205 and 207 are not claimed in claim 20 because they take place in the network, for instance in the software provider server 125 of Fig. 1. The receiving step corresponding to reference numeral 209 of Fig. 2 takes place in the terminal.

Nothing like these kinds of steps of transmitting and receiving are shown between the base station 20 and the terminal 10 of *Geiger*. The only thing that is described is the possible download of an applet in step 201 of Fig. 3.

In contrast, the present disclosure in Figure 2 shows a transmit step 203 in which identifying information concerning the terminal (such as an IMEI) and the memory unit (such as an MMC serial number) are transmitted to the software provider.

Claim 20 being directed to a method that takes place in the communication terminal 101 of Fig. 1, for example, it does not claim that which is shown in steps 205 and 207 of Figure 2. However, for better understanding of what takes place in the terminal, these steps that are carried out in the network involve for instance the software provider checking if it really is the issuer or provider of an MMC 103 with the particular MMC serial number containing the software module corresponding to a hash value sent by the communication terminal. If it succeeds in making a match, it digitally signs the received info and the server then returns the result in a key file to the communication terminal. Also not claimed in claim 20 but helpful for understanding claim 20 is the step of the software provider server storing the MMC serial number relationship in its database so that the provider will not permit itself to sign any other, i.e., later request for the same MMC serial number and same software module.

Again, the step 209 takes place in the terminal and receives the digitally signed data block (key file) comprising a reference value for use during integrity checking of the software module which allows the software module to take control

of the terminal only if the integrity of the software module properly checks. This is shown for instance in Figure 3 where after a hashing step 301 is carried out the result is checked in step 303 as to whether or not the hash value matches the received reference value (see page 9, lines 22-35 and continuing on to page 10, line 3) (see also published application US 2004/0111618 at paragraphs 0036-0038).

Thus, properly understood, the transmitting and receiving steps 203 and 209 of Figure 2 as claimed in claim 20 are part of a process which ends up enabling the integrity checking of the software as shown in Figure 3. Thus, the transmitting and receiving steps of claim 20 correspond to the steps 203 and 209 of Figure 2 and the checking step 303 of Fig. 3 corresponds to the last step of claim 20 which claims that the software module is allowed to take control of the terminal only if the integrity of the software module properly checks.

The invention as claimed and described above provides a simple and effective way of enabling an integrity check of a software module as explained in detail beginning at page 10, line 4 and continuing through page 10, line 29 (see paragraph 0039-0043 of the published application).

Referring back to the *Geiger* reference, it will now be more clearly realized that the illustration of Figure 2 of *Geiger* is a flow diagram of a process performed by an issuer of a subscriber identity module which is performed by the entity issuing this SIM to the subscriber when a subscriber is physically issued with the SIM. This does not take place by virtue of any "communication" via a mobile communication system with a software provider as alleged by the Examiner. Rather, this takes place at the time the SIM card is handed over to the subscriber. The hashed value is at that time (or prior thereto) loaded on to the SIM card by the issuer and there it resides as a "fingerprint" of an executable object. See page 4, line 22 through page 5, line 17.

It will further be appreciated that the steps shown in Figure 3 of *Geiger*, except for step 201, all take place within the mobile station in which the hashed value of the executable object 101 is already stored on the SIM card 102 by virtue of

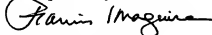
the issuer of the SIM card already having stored this on the SIM card at the time of issuance. When the application is launched in step 201 or the applet is downloaded, a hash is created of the application or the applet in step 202. Then a list is checked that is residing on the SIM card to find out if it should be checked or not. If so, it is verified in a step 220 against the previously stored hash value stored by the SIM issuer in step 102. So, there is no transmit step 203 and receive step 209 such as shown in Fig. 2 of the present application in the *Geiger* reference.

It will thus be realized that the fundamental nature of the presently claimed invention is not at all comparable to what is shown by *Geiger* for the above reasons.

The *Proust et al* reference seems only to describe a SIM card, which relevance is not particularly an issue in this application in view of the foregoing remarks. The Examiner uses the reference to disclose the "missing features" of *Geiger*, which the Examiner believes to be a removable unit having associated memory card identity information. However, the foregoing considerations have shown that the *Geiger* reference is missing much more than the memory card aspect and it is respectfully believed that the Examiner will be persuaded that the previous analysis is not correct and will withdraw the obviousness rejection for the above reasons. Therefore, in view of the above remarks, the Examiner is respectfully requested to withdraw the obviousness rejection of claims 20-23 and allow the case.

The objections and rejections of the Office Action of July 31, 2007, having been obviated by amendment or shown to be inapplicable, withdrawal thereof is requested and passage of claims 20-23 to issue is solicited.

Respectfully submitted,



Francis J. Maguire
Attorney for the Applicant
Registration No. 31,391

FJM/ik
WARE, FRESSOLA, VAN DER SLUYS
& ADOLPHSON LLP
755 Main Street, P.O. Box 224
Monroe, Connecticut 06468
(203) 261-1234